Hacker Stories: Turning Use Cases Into Abuse Cases

Steve Ocepek
X-Force Red CTO

X-Force Red

IBM

Who am I?

I am an executive hacker.


X-Force Red

Hacking Anything to Secure Everything

X-Force Red is an autonomous team of veteran hackers, within IBM Security, hired to break into organizations and uncover vulnerabilities that criminals may use for personal gain.

Penetration Testing

Test your applications, networks, hardware, personnel and more to uncover and fix vulnerabilities

Adversary Simulation

Simulate real-world attacks and measure your security team's response

Vulnerability Management

Rank and remediate vulnerabilities targeting your most important assets

X-Force Red

IBM

X-Force Red CTO Steve Ocepek hugging his favorite house plant

X-Force Red hacker Dan Crowley picking his first lock at 4-years-old

X-Force Red is different

Real-time view into testing programs with the X-Force Red Portal. Clients see and remediate vulnerabilities as they are uncovered.

SKILLS

Hack anything criminals can hack

Decades of hacking experience professionally and personally

Manual penetration testing virtually and physically, no questionnaires

Engineers and **developers** who also have security expertise

SCALE

Automated Vulnerability prioritization based on **weaponization** and asset value

Fixed price with subscription testing program.

SCOPE

Four secure, global "X-Force Red Labs" for **IoT, IIoT, OT testing**

ATM Testing service

Red teaming service separate from penetration testing

What is hacking?

Hacking is: Problem Solving

- Trying to make something do something it can't
- Getting to know a system so intimately you can work around its perceived limitations
- Making the most of access rights and limited resources

Why do vulnerabilities matter?

1.7m

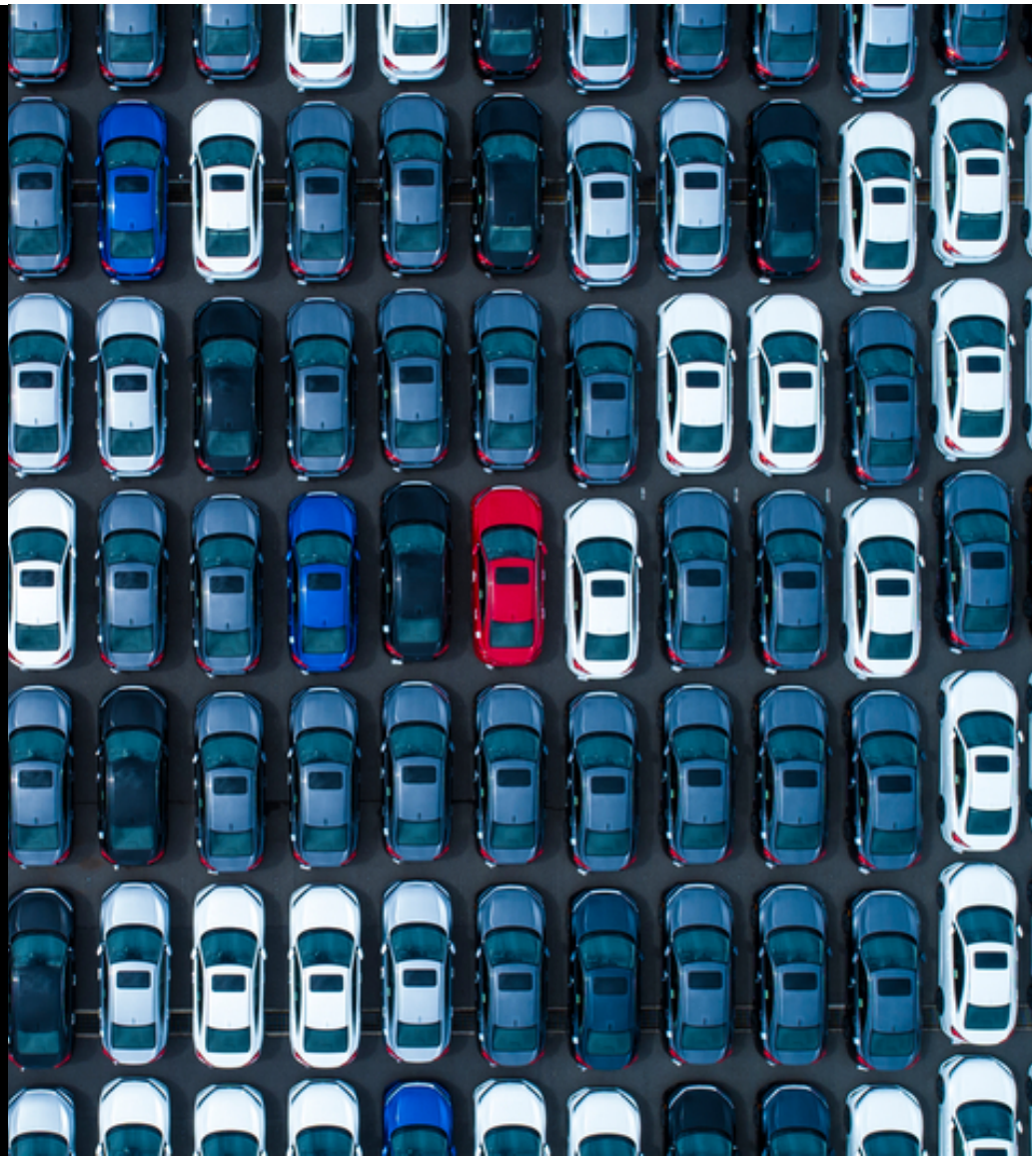
Average number of vulnerabilities reported by scanners in enterprise client environments at any point in time

Source: X-Force Red Client Statistical Analysis

16%

Percentage of vulnerabilities that have associated public exploits

Source: X-Force Red Client Statistical Analysis



Why does the world focus on use cases?

Humans focus on the activities that they can relate to carrying out themselves.

When people look at a widget, we see the widget as they would be likely to use it.

Developers often have issues envisioning the use cases of a product and have specific design thinking activities to flesh out use cases they may not immediately see.

The value of function is often subjective.

The hacker approach to problem solving is often unique.

While most people are focused on using things in the intended manner, the hacker is focused on making something work in a way it was never intended.

The guard rails of intended use of a widget often leave open a wide array of unintended uses.

The value of unintended use is often extremely high.

There is nothing wrong with using a butter knife as a screwdriver unless you have a Phillips head screw.

How do use cases compare to abuse cases?

Example One: Frequent Fliers

Use cases for airlines:

- Frequent flier numbers establish unique identifiers for VIP customers
- Including frequent flier on boarding passes allows for easier determination of status benefits
- Including record locators on boarding passes allows for them to easily be passed between airlines
- Basic passenger details are required to be on boarding passes by the TSA

Example One: Frequent Fliers

Use cases for airlines:

- Frequent flier numbers establish unique identifiers for VIP customers
- Including frequent flier on boarding passes allows for easier determination of status benefits
- Including record locators on boarding passes allows for them to easily be passed between airlines
- Basic passenger details are required to be on boarding passes by the TSA

Use cases for fliers:

- Frequent flier numbers and programs allow fliers to earn rewards
- Status allows frequent fliers to board the plane early, check free bags, and earn upgrades.
- Frequent flier programs tie nicely to airline system accounts. This easily enables frequent fliers to track, maintain, and retrieve flight information across multiple systems.

Example One: Frequent Fliers

Use cases for airlines:

- Frequent flier numbers establish unique identifiers for VIP customers
- Including frequent flier on boarding passes allows for easier determination of status benefits
- Including record locators on boarding passes allows for them to easily be passed between airlines
- Basic passenger details are required to be on boarding passes by the TSA

Use cases for fliers:

- Frequent flier numbers and programs allow fliers to earn rewards
- Status allows frequent fliers to board the plane early, check free bags, and earn upgrades.
- Frequent flier programs tie nicely to airline system accounts. This easily enables frequent fliers to track, maintain, and retrieve flight information across multiple systems.

Abuse case for attackers:

The information required to retrieve or alter a reservation is the same information on the boarding pass. This same information can often (depending on airline) be used to reset account passwords.

These boarding passes are often left in seat back pouches or airport trashcans. Frequent fliers are often oblivious to the value of the information they leave behind.

Example Two: SMS Authentication

Use cases for developers:

- SMS authentication provides an easy method for two-factor authentication and password resets.
- The ubiquitous nature of mobile phones today provides an almost guaranteed availability of SMS for almost all users.
- SMS authentication often meets compliance requirements.

Example Two: SMS Authentication

Use cases for developers:

- SMS authentication provides an easy method for two-factor authentication and password resets.
- The ubiquitous nature of mobile phones today provides an almost guaranteed availability of SMS for almost all users.
- SMS authentication often meets compliance requirements.

Use cases for users:

- SMS authentication is fairly simple for even novice users.
- Users generally carry their phone with them at all times and, in many cases, use their phones more than computers or other devices which may require authentication.

Example Two: SMS Authentication

Use cases for developers:

- SMS authentication provides an easy method for two-factor authentication and password resets.
- The ubiquitous nature of mobile phones today provides an almost guaranteed availability of SMS for almost all users.
- SMS authentication often meets compliance requirements.

Use cases for users:

- SMS authentication is fairly simple for even novice users.
- Users generally carry their phone with them at all times and, in many cases, use their phones more than computers or other devices which may require authentication.

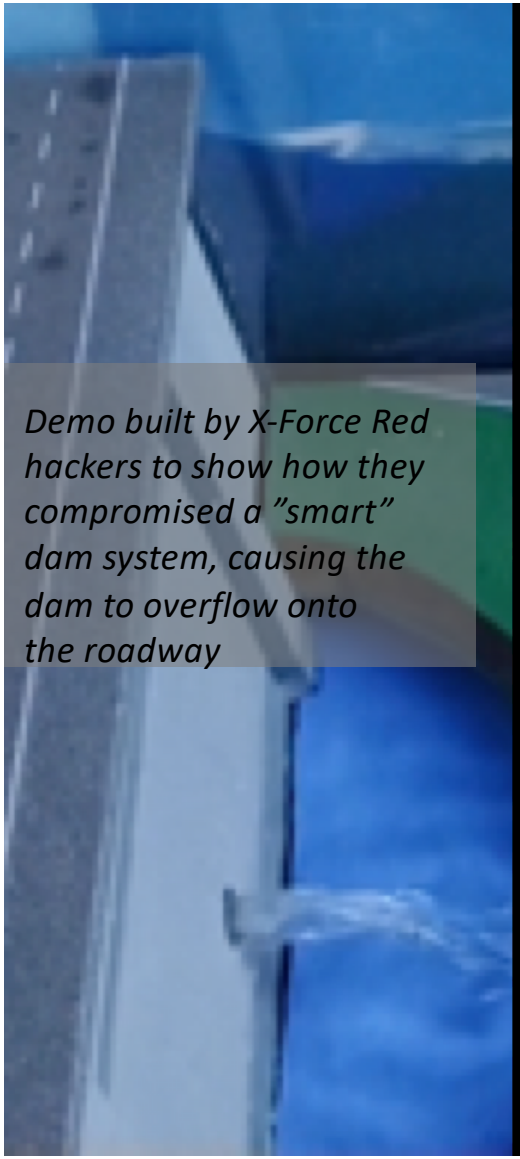
Use case for attackers:

SIM Swapping

SIM Swapping: A Deeper Dive

Cities are smart!

- Smart technology allows city employees to manage infrastructure remotely at a much lower cost.
- What once required onsite maintenance can now be done quickly and cheaply.
- Infrastructure monitoring devices allow city staff to learn of issues before they become problems.



Demo built by X-Force Red hackers to show how they compromised a "smart" dam system, causing the dam to overflow onto the roadway

Technology, not so much...

X-Force Red found 17 zero-day vulnerabilities within four smart city products. Research unveiled at Black Hat USA 2018. Landed 100+ media stories worldwide.

BBC

WIRED

eWEEK

CNBC

Forbes

WSJ PRO CYBERSECURITY

THE PARALLAX
YOUR EYE ON SECURITY NEWS

CNN

FOX BUSINESS

The Washington Post

So, what should you do?

- Just as you brainstorm to flesh out use cases, critically discuss possible abuse cases with developers, executives, and outsiders.
- Plan for abuse and conduct threat modeling.
- Have a third-party test extensively and manually to ensure that your solution is vetted.
- Understand that the worst possible scenario is likely the scenario you do not consider.

Questions?

Thank you

Follow us on:

ibm.com/xforcered

@xforcered

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

youtube.com/ibmsecurity

X-Force Red

IBM